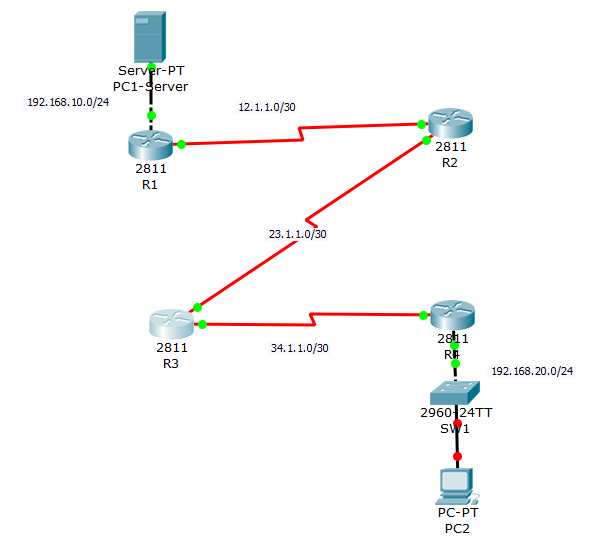
**LAB 11: Configuring ACL to mitigate Attacks**

**Topology:**

****

**IP Address Table**

**Step 1:**

Configuring IP on all interfaces

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Description |
| R1 | S0/0/0 | 12.1.1.1 | 255.255.255.252 | Link to R2 |
| Fa0/0 | 192.168.10.1 | 255.255.255.0 | Link to Server |
| R2 | S0/0/0 | 12.1.1.2 | 255.255.255.252 | Link to R1 |
| S0/0/1 | 23.1.1.1 | 255.255.255.252 | Link to R3 |
| R3 | S0/0/0 | 34.1.1.1 | 255.255.255.252 | Link to R4 |
| S0/0/1 | 23.1.1.2 | 255.255.255.252 | Link to R2 |
| Loopback | 192.168.30.1 | 255.255.255.0 | Loopback Address |
| R4 | S0/0/0 | 34.1.1.2 | 255.255.255.252 | Link to R3 |
| Fa0/0 | 192.168.20.1 | 255.255.255.0 | Link to SW1 |
| PC1 | F0 | 192.168.10.2 | 255.255.255.0 |  |
| PC2 | F0 | 192.168.20.2 | 255.255.255.0 |  |

Objectives

* Verify connectivity among devices before firewall configuration.
* Use ACLs to ensure remote access to the routers is available only from management station PC2.
* Configure ACLs on R1 and R4 to mitigate attacks.
* Verify ACL functionality.

Introduction

Access to routers R1, R2, R3 and R4 should only be permitted from PC2, the management station. PC2 is also used for connectivity testing to PC1-SERVER, a server providing DNS, SMTP, FTP, and HTTPS services.

Standard operating procedure is to apply ACLs on edge routers to mitigate common threats based on source and/or destination IP address. In this activity, you create ACLs on edge routers R1 and R4 to achieve this goal. You then verify ACL functionality from internal and external hosts.

The routers have been pre-configured with the following:

* Enable password: **ciscoenable**
* Password for console: **ciscoconsole**
* Username for VTY lines: **ssh**
* Password for VTY lines: **passssh**
* IP addressing
* RIP routing

1. Verify Basic Network Connectivity – 20points

Verify network connectivity prior to configuring the IP ACLs.

**Step1.** From the PC2 command prompt, ping the PC1-SERVER server.

**Step2.** From the PC2 command prompt, SSH to the router R3 Lo0 interface. Exit the SSH session.

**Step 3.** From PC2, open a web browser to the PC1-SERVER server (using the IP address : 192.168.10.2) to display the web page. Close the browser on PC2.

**Step 4.** From the PC1-SERVER server command prompt, ping PC2.

Task2: Secure Access to Routers – 20points

Step1. Configure ACL 11 to block all remote access to the routers except from PC2.

Use the **access-list** command to create a numbered IP ACL on R1, R2, R3 and R4.

R1(config)# access-list 11 permit host 192.168.20.2

R2(config)# access-list 11 permit host 192.168.20.2

R3(config)# access-list 11 permit host 192.168.20.2

R4(config)# access-list 11 permit host 192.168.20.2

Step 2. Apply ACL 11 to ingress traffic on the VTY lines.

Use the **access-class** command to apply the access list to incoming traffic on the VTY lines.

R1(config)#line vty 0 4

R1(config-line)#access-class 11 in

R2(config)#line vty 0 4

R2(config-line)#access-class 11 in

R3(config)#line vty 0 4

R3(config-line)#access-class 11 in

R4(config)#line vty 0 4

R4(config-line)#access-class 11 in

Step 3. Verify exclusive access from management station PC2.

SSH to 192.168.30.1 from PC2 (should be successful). SSH to 192.168.30.1 from PC1-SERVER (should fail).

PC> ssh -l ssh 192.168.30.1

Task 3: Create a Numbered IP ACL 111 -20points

On R4, block all packets containing the source IP address from the following pool of addresses: 127.0.0.0/8, any RFC 1918 private addresses, and any IP multicast address.

Step1. Configure ACL 111 to block all specified traffic from the outside network.

You should also block traffic sourced from your own internal address space if it is not an RFC 1918 address (in this activity, your internal address space is part of the private address space specified in RFC 1918).

Use the **access-list** command to create a numbered IP ACL.

R4(config)#access-list 111 deny ip 10.0.0.0 0.255.255.255 any

R4(config)#access-list 111 deny ip 172.16.0.0 0.15.255.255 any

R4(config)#access-list 111 deny ip 192.168.0.0 0.0.255.255 any

R4(config)#access-list 111 deny ip 127.0.0.0 0.255.255.255 any

R4(config)#access-list 111 deny ip 224.0.0.0 15.255.255.255 any

R4(config)#access-list 111 permit ip any any

Step2. Apply the ACL to interface Serial 0/0/0.

Use the **ip access-group** command to apply the access list to incoming traffic on interface Serial 0/0/0.

R4(config)# interface S0/0/0

R4(config-if)#ip access-group 111 in

Step3. Confirm that the specified traffic entering interface Serial 0/0/0 is dropped.

From the PC2 command prompt, ping the PC1-SERVER server. The ICMP echo *replies* are blocked by the ACL since they are sourced from the 192.168.0.0/16 address space.

Step 4. Remove the ACL from interface Serial 0/0/0.

Remove the ACL. Otherwise, all traffic from the outside network (being addressed with private source IP addresses) will be denied for the remainder of the PT activity.

Use the **no ip access-group** command to remove the access list from interface Serial 0/0/0.

R4(config)# interface s0/0/0

R4(config-if)# no ip access-group 111 in

**Note:** In order for the PT activity to score 100 percent, the ACL needs to be grouped to the interface at the end of the activity:

R3(config)# interface s0/0/0

R3(config-if)# ip access-group 111 in

Task 4: Create a Numbered IP ACL 122 – 20points

Deny all outbound packets with source address outside the range of internal IP addresses.

Step 1. Configure ACL 122 to permit only traffic from the inside network.

Use the **access-list** command to create a numbered IP ACL.

R4(config)#access-list 122 permit ip 192.168.20.0 0.0.0.255 any

Step 2. Apply the ACL to interface F0/0.

Use the **ip access-group** command to apply the access list to incoming traffic on interface F0/0.

R4(config)#interface Fa0/0

R4(config-if)#ip access-group 122 in

Create a Numbered IP ACL 133

Permit any outside host to access DNS, SMTP, and FTP services on server PC1-SERVER, deny any outside host access to HTTPS services on PC1-SERVER, and permit PC2 to access R1 via SSH.

Step 1. Verify that PC2 can access the PC1-SERVER via HTTPS using the web browser.

Be Task 5: sure to disable HTTP and enable HTTPS on server PC1-SERVER.

Step 2. Configure ACL 133 to specifically permit and deny the specified traffic.

Use the **access-list** command to create a numbered IP ACL.

R1(config)#access-list 133 permit udp any host 192.168.10.2 eq domain

R1(config)#access-list 133 permit tcp any host 192.168.10.2 eq smtp

R1(config)#access-list 133 permit tcp any host 192.168.10.2 eq ftp

R1(config)#access-list 133 deny tcp any host 192.168.10.2 eq 443

R1(config)#access-list 133 permit tcp host 192.168.20.2 host 12.1.1.1 eq 22

Step 3. Apply the ACL to interface S0/0/0.

Use the **ip access-group** command to apply the access list to incoming traffic on interface S0/0/0.

R1(config)# interface s0/0/0

R1(config-if)# ip access-group 133 in

Step 4. Verify that PC2 cannot access PC1-SERVER via HTTPS using the web browser.

Task 5: Modify An Existing ACL – 20points

Permit ICMP echo replies and destination unreachable messages from the outside network (relative to R1); deny all other incoming ICMP packets.

Step 1. Verify that PC1-SERVER cannot successfully ping the loopback interface on R2.

Step 2. Make any necessary changes to ACL 133 to permit and deny the specified traffic.

Use the **access-list** command to create a numbered IP ACL.

R1(config-if)#access-list 133 permit icmp any any echo-reply

R1(config)#access-list 133 permit icmp any any unreachable

R1(config)#access-list 133 deny icmp any any

R1(config)#access-list 133 permit ip any any

Step 3. Verify that PC1-SERVER can successfully ping the loopback interface on R3.